(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: **0 095 272**
A1

(12) EUROPEAN PATENT APPLICATION

(21) Application number: 83302593.5

(22) Date of filing: 09.05.83

(51) Int. Cl.³: G 06 F 7/58

(30) Priority: 21.05.82 GB 8214945

(43) Date of publication of application:
30.11.83 Bulletin 83/48

(84) Designated Contracting States:
AT BE CH DE FR IT LI LU NL SE

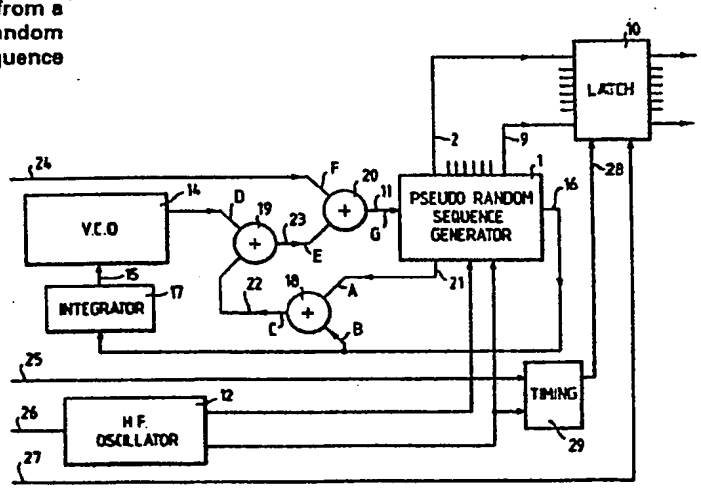
(71) Applicant: THE MARCONI COMPANY LIMITED
The Grove Warren Lane
Stanmore Middlesex HA7 4LY(GB)

(72) Inventor: Jenner, Peter Michael
19 Craneswater Avenue
Southsea Hampshire(GB)

(74) Representative: Dolwin, John Davison
Central Patent Department The General Electric
Company plc Hirst Research Centre East Lane
Wembley Middlesex HA9 7PP(GB)

(54) Random sequence generators.

(57) A pseudo-random sequence generator has two oscillators, the first of which controls the rate of stepping through the pseudo-random sequence and the second of which controls selection of the sequence and the inverse of the sequence. By replacing the second oscillator with a voltage controlled oscillator and deriving the control voltage from a decaying integration of at least one output of the random sequence generator (or another pseudo-random sequence generator) a near-true digital noise is produced.



EP 0 095 272 A1

Croydon Printing Company Ltd

The present invention relates to random sequence generators and more particularly to such generators the output electrical signals of which represent in digital form an apparently random sequence of multi digit numbers.

Pseudo random sequence generators, which now are well known, use clock signals from high frequency oscillators, which may be self contained in the generator, to step through a long series of output changes representing a pseudo-random sequence of multi-digit numbers. After a period of time the sequence will recommence.

In order to extend the range of the pseudo-random sequence it is also known to disturb the logic state of the generator by periodically altering the feedback of the generator using a second oscillator having a lower frequency.

The random time jitter between the two oscillator periods results in a further small variation in the number sequence produced.

It is an object of the present invention to increase the variation in the number sequence produced such that the output of the random sequence generator approaches a true random digital noise source.

According to one aspect of the present invention in a method of controlling a pseudo-random generator of the kind which steps through a pseudo-random sequence in response to periodic clock signals received from a first oscillator and which is responsive to clock signals received from a second oscillator to cause a change in the pseudo-random sequence, the periodicity of the clock signals supplied by the second oscillator is varied in dependance upon a decaying integration of the value of an output of the pseudo-random sequence generator.

According to a second aspect of the present invention in a random sequence generator, a pseudo-random sequence generator which is responsive to periodic clock signals from a first oscillator to step through a pseudo-

random sequence and which is responsive to clock signals received from a second oscillator to cause a change in the pseudo-random sequence, and the periodicity of the clock signals supplied by the second oscillator is controlled in dependance upon a decaying integration of the value of an output of the pseudo-random sequence generator.

Preferably said second oscillator is a voltage controlled oscillator and an output of the pseudo-random number generator is integrated by an integrator to provide the voltage to control the frequency output thereof.

A further input may be provided to the pseudo-random sequence generator to cause in combination with the clock signals from the second oscillator further variations in the changes of the pseudo-random sequence.

The output of the random sequence generator may be fed to a latch which may be arranged to receive clock pulses at periodic intervals to store the output of the pseudo-random sequence generator from time to time. The output of the latch may be in binary form or may be arranged to respond to a further signal to provide a tristate output.

A random sequence generator in accordance with the invention will now be described by way of example only with reference to the accompanying drawing which is a block diagram of the generator.

Referring to the drawing the generator comprises a pseudo-random sequence generator 1 providing an eight bit output on leads 2 to 9 which are connected to a latch 10. In the absence of a change in a control signal on an input 11, the pseudo-random sequence generator 1 steps through every possible combination of the eight outputs 2-9 in a predetermined (pseudo-random) order under control of clock signals supplied by a frequency oscillator 12.

It will be appreciated that in one condition of the input 11 (say logic '0') the pseudo-random sequence

generator 1 steps through the predetermined order of the outputs 2-9 whilst in the other condition (logic 1) of the input 11 the inverse of the sequence is provided.

Accordingly it is known to use a second oscillator connected to the input 11 to cause switching between the primary random sequence and the inverse of the sequence. The second oscillator has a lower frequency than the oscillator 12 and the presence of a random time jitter between the two oscillators introduces a small further random element into the sequence due to a variation of plus or minus one in the number of high frequency oscillator periods in one period of the low frequency oscillator.

In the present circuit the low frequency oscillator is replaced by a voltage controlled oscillator 14 the output frequency of which varies in response to the voltage at an input 15. The voltage applied at the input 15 is derived from one output 16 of the pseudo-random sequence generator 1 which output may be one of the outputs 2-9 or a separately controlled output of the generator 1. The output 16 is connected to an integrator circuit 17 which has a fixed time constant. Thus the value of the voltage provided by the integrator 17 commences at zero and increases each time a '1' is present at the output 16, with the voltage value decreasing at a constant rate when an '0' is present at the output 16. Thus the frequency of the oscillator varies continuously in dependance upon the signal at the output 16 and the time constant of the integrator 17 and, if the oscillator is directly connected to the input 11 of the pseudo-random sequence generator 1 the output sequence will switch to the inverse sequence at periodic intervals.

Each time one condition (say logic '1') is present at the output 16 the voltage output of the integrator 17 will increase and the frequency of the oscillator 14 will increase accordingly at varying rates since the output 16

is also responding to the changes caused by the feedback to the pseudo-random sequence generator 1. Thus a continuously varying interchange between the two sequences of the pseudo-random sequence generator 1 occurs due to the variation in the disturbance pattern applied to the input 11.

To cause a further variation in the disturbance pattern a number of EXCLUSIVE OR (EXOR) logic gates 18 to 20 are provided. The EXOR gate 18 has one of its two inputs connected to the output 16 and the other of its inputs connected to a further output 21 (which may be one of the outputs 2-9) of the pseudo-random number generator 1.

The output 22 of the EXOR gate 18 is connected to one of the two inputs of the EXOR gate 19 the other of which is connected to the output of the voltage controlled oscillator 14. The output 23 of the EXOR gate 19 is connected to one input of the EXOR gate 20 the other input of which is connected as an external input 24 to the random number generator.

A further disturbance pattern influence, such as another random number generator, may be connected to the input 24. Thus it will be appreciated that the random pattern at the outputs 2 to 9 of the pseudo-random sequence generator 1 is approaching a true random digital noise source.

The latch 10 may be a three-state D-type latch which when enabled by way of an input 27 provides a tri-state output from the binary input suitable for connection to equipment requiring such an input. When no signal is present on the input lead 27 the random output present on the leads 2-9 at the time a clock signal is present on the input 28 is stored and presented at the output.

To enable the output to be latched timing signals may be presented at an input 25 of the random sequence

generator. On receipt of a timing signal on the lead 25 a timing circuit 29 awaits the next clock signal from the oscillator 12 before forwarding a signal to the input 28 of the latch.

The latch may alternatively be controlled to provide a serial output signal from the parallel input signal provided by the pseudo-random number generator 1.

The random number generator may be suitably implemented in a thick film hybrid integrated circuit.

It will be realised that whilst as herein described the voltage at the input 15 of the voltage controlled oscillator 14 is derived from an output of the pseudo-random sequence generator 1, the voltage may be derived from any suitable source. For example the integrator 17 may be supplied by signals from a further pseudo-random sequence generator (not shown).

The invention finds particular use in the field of cryptography but may be of use in any field in which high quality random number generation is required. Examples of such fields include gambling and lotteries.

CLAIMS

1. A method of controlling a pseudo-random sequence generator of the kind which steps through a pseudo-random sequence in response to periodic clock signals received from a first oscillator and which is responsive to a second oscillator to cause a change in the pseudo-random sequence wherein the periodicity of the clock signals supplied by the second oscillator is varied in dependance upon a decaying integration of the value of another pseudo-random sequence.

2. A method according to Claim 1 in which the other pseudo-random sequence is derived from an output of the controlled pseudo-random sequence generator.

3. A random sequence generator of the kind having a pseudo-random sequence generator (1) which is responsive to periodic clock signals from a first oscillator (12) to step through a pseudo-random sequence and which is responsive to clock signals from a second oscillator (14) to cause a change in the pseudo-random sequence characterised in that the periodicity of the clock signals supplied by the second oscillator (14) is controlled in dependance upon a decaying integration of the value of another pseudo-random sequence.

4. A random sequence generator according to Claim 3 wherein said other pseudo-random sequence is derived from an output (16) of the random sequence generator.

5. A random sequence generator according to Claim 3 or Claim 4 wherein said second oscillator (14) is a voltage controlled oscillator and said other pseudo-random sequence is integrated by an integrator (17) to provide the voltage to control the output frequency thereof.

6. A random sequence generator according to Claim 3, Claim 4 or Claim 5 in which means (20) are provided to

combine the clock signals from the second oscillator (14) with signals from an external source to cause further variations in the pseudo-random sequence.

7. A random sequence generator according to Claim 6 in which the external source is another pseudo-random or random sequence generator.

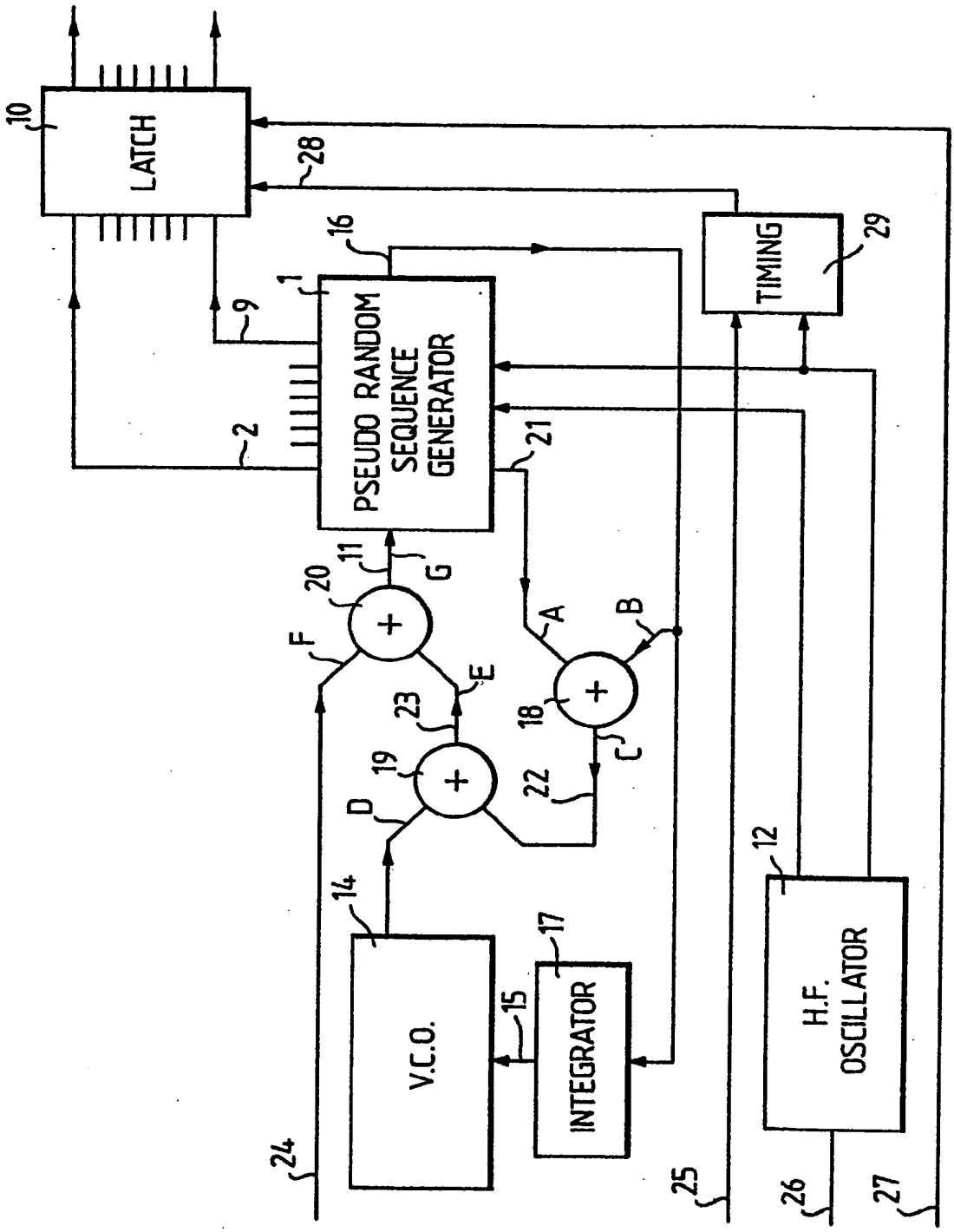
8. A random sequence generator according to any one of Claims 3 to 7 in which means (18, 19) are provided to combine the clock signals from the second oscillator (14) with signals derived from an output or outputs (16,21) of the random sequence generator to cause further variations in the pseudo-random sequence.

9. A random sequence generator according to any one of Claims 3 to 8 in which the output of the pseudo-random sequence generator (1) is fed to a latch (10) which is responsive to clock pulses at an input (28) to store the output of the pseudo-random sequence generator from time to time.

10. A random sequence generator according to Claim 9 in which the output of the latch (10) represents a binary word.

11. A random sequence generator according to Claim 9 in which the latch is responsive to a further signal at an input (27) thereof to provide a tri-state output.

12. A random sequence generator according to Claim 9, Claim 10 or Claim 11 in which the latch is arranged to provide the output pseudo-random sequence in serial form.



European Patent Office

EUROPEAN SEARCH REPORT

0095272
Application number

EP 83 30 2593

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl. ³)
Y	DE-A-2 829 293 (GLITZ) * Claim 6; figures 1-3,7; page 4, lines 1-5; page 6, last paragraph - page 7, first paragraph; page 8, one before last paragraph - page 9, last paragraph *	1-4,6-8	G 06 F 7/58
Y	ELECTRONICS LETTERS, vol. 3, no. 2, February 1967, pages 88-90, Hitchin, GB. M. DARNELL: "Generation of quadratic-residue sequences" * Figure 1; page 88, right-hand column, last paragraph - page 88, right-hand column, first paragraph *	1-4	
A	US-A-3 681 708 (OLMSTEAD)	1,3	TECHNICAL FIELDS SEARCHED (Int. Cl. ³)
A	FR-A-2 239 817 (BREANT)	1,3	G 06 F 7/58
A	US-A-4 161 041 (BUTLER et al.)	1,3	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	08-09-1983	FORLEN G.A.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO Form 1503. 03.82